Allegato P)

Procedura “Data Breach”

Regolamento UE 679/2016

SOMMARIO

1. SCOPO

Scopo della procedura è definire le modalità e le responsabilità per effettuare:

- la notifica di una violazione dei dati personali all'autorità di controllo;
- la comunicazione di una violazione dei dati personali all'interessato;

garantendo altresì:

- l’identificazione della violazione;
- l’analisi delle cause della violazione;
- la definizione delle misure da adottare per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;
- la registrazione delle informazioni relative alla violazione, delle misure identificate e dell'efficacia delle stesse.

2. CAMPO DI APPLICAZIONE

La procedura è applicabile a tutte le attività svolte da Formez PA, (di seguito il titolare del trattamento), con particolare riferimento alla gestione di tutti gli archivi/documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati (clienti, fornitori, altri soggetti terzi, ecc.), anche con il supporto di fornitori esterni.

3. DEFINIZIONI E ABBREVIAZIONI

3.1. Definizioni

Per l'elenco completo, si rimanda all'Art. 4 del REGOLAMENTO (UE) 2016/679

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali,

come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia,

le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «Autorità di controllo/Autorità»: l'autorità pubblica indipendente istituita da uno Stato membro; in Italia è il Garante per la protezione dei dati personali.

3.2. Abbreviazioni

RPD Responsabile per la protezione dei dati personali

RTDP Responsabile della tutela dei dati personali e della sicurezza dei dati aziendali

RAID Responsabile Area innovazione digitale

4. RESPONSABILITÀ

RAID
- Segnalazione a RPD delle violazioni rilevate su dati digitalizzati e archiviati su sistemi, dotazioni informatiche e siti aziendali gestiti dal Sistema informativo Formez PA e raccolta delle informazioni tecniche su di essa

RPD
- Gestione della procedura Data Breach dalla notifica al Garante alla chiusura con la fornitura di tutte le informazioni richieste

RTDP
- Supervisione della procedura

5. MODALITÀ ESECUTIVE

5.1. Individuazione della violazione

Le violazioni dei dati personali sono una tipologia di incidente per la sicurezza delle informazioni nel quale sia coinvolto qualsiasi genere di dato di natura personale (anagrafici, numeri di carte personali, codici identificativi, dati sanitari, dati biometrici, dati relativi a conti correnti, ecc.).

Le violazioni dei dati personali possono essere classificate in base ai seguenti tre principi di sicurezza delle informazioni:

- Violazione della riservatezza – in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- Violazione dell'integrità – in caso di alterazione non autorizzata o accidentale dei dati personali;
- Violazione della disponibilità – in caso di accidentale o non autorizzata perdita di accesso o distruzione di dati personali.

A seconda delle circostanze, una violazione può riguardare tutti gli aspetti sopra indicati o una combinazione di essi.

Tutti possono rilevare violazioni dei dati personali (di seguito “violazioni”).

5.2. Segnalazione della violazione

5.2.1. Violazione di dati digitalizzati

Nel caso la violazione interessi dati archiviati in formato digitale su basi dati o supporti di memorizzazione messi a disposizione dal sistema informativo di Formez PA devono essere osservate le seguenti modalità per la segnalazione.

1. Chi rileva la violazione lo comunica a **RAID** e per conoscenza a **RPD** fornendo i dati in suo possesso presenti nel modello semplificato in Allegato 5.
2. RAID accerta la reale esistenza della violazione e, in caso sia confermata la violazione stessa, conferma a RPD l’avvenuta violazione.
3. RPD, acquisito un ragionevole grado di certezza del fatto che sia avvenuta un incidente per la sicurezza delle informazioni che abbia compromesso dati personali, inserisce una voce per la descrizione del data breach nel “Registro delle violazioni”, come indicato al § 5.5 ed avvia il trattamento della violazione come descritto nelle sezioni successive 5.3 e 5.4.

In Allegato 4 “Scenari di Data Breach” è riportato un elenco esemplificativo di eventi da cui possono derivare violazioni dei dati personali, con indicazione della necessità di notifica e di comunicazione.

5.2.2. Violazione di dati su supporti fisici o informatizzati personali

Nel caso la violazione interessi archivi o documenti cartacei o informazioni digitalizzate contenute su supporti fisici di memorizzazione non gestiti dal sistema informativo di Formez PA devono essere osservate le seguenti modalità per la segnalazione.

1. Chi rileva la violazione lo comunica a **RPD** fornendo i dati in suo possesso presenti nel modello semplificato in Allegato 5.
2. RPD, acquisito un ragionevole grado di certezza del fatto che sia avvenuta un incidente per la sicurezza delle informazioni che abbia compromesso dati personali,

inserisce una voce per la descrizione del data breach nel “Registro delle violazioni”, come indicato al § 5.5 ed avvia il trattamento della violazione come descritto nelle sezioni successive 5.3 e 5.4.

5.3. Valutazione del rischio connesso alla violazione

Per identificare le modalità di gestione di una violazione e gli eventuali obblighi di notifica e/o di comunicazione, RPD (con il supporto di RAID nel caso di dati digitalizzati gestiti dal sistema informativo Formez PA) effettua la valutazione del rischio, come di seguito indicato.

Il livello di rischio è definito sulla base di due parametri, gravità e probabilità:

- gravità: rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell’interessato sulla diffusione dei propri dati);
- probabilità: grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, è possibile considerare i seguenti fattori:

- tipo di violazione, secondo quanto specificato al § 5.1;
- natura, sensibilità e volume dei dati personali;
- facilità nella identificazione degli interessati;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati (es. bambini);
- particolarità dei responsabili del trattamento (es. personale sanitario);
- numero degli interessati.

Gravità	Impatto della violazione sui diritti e le libertà delle persone coinvolte: • Basso: nessun impatto • Medio: impatto poco significativo, reversibile • Alto: impatto significativo, irreversibile
Probabilità	Possibilità che si verifichino uno o più eventi temuti • Basso: l'evento temuto non si manifesta • Medio: l'evento temuto potrebbe manifestarsi • Alto: l'evento temuto si è manifestato

	Gravità			
		A	M	B
Probabilità	A			
	M			
	B			

	Descrizione	Notifica all’Autorità	Comunicazione agli interessati
Rischio	Basso: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	NO	NO
	Medio: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	NO
	Alto: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	SI

Sulla base degli elementi di cui sopra:

1. RPD stima la gravità e la probabilità della violazione e classifica il rischio;
2. RPD, previa condivisione della valutazione con RTDP, documenta la decisione presa a seguito della valutazione del rischio nel “Registro delle violazioni”
    a. Nel caso in cui il rischio sia considerato non elevato e non si ritenga necessario procedere con la comunicazione, RPD specifica la giustificazione per tale scelta.

b. Nel caso il rischio lo richieda, RPD procede alla notifica della violazione (§ 5.4)

3. Gli elementi a supporto del procedimento e degli esiti della valutazione del rischio sono documentati da RPD e tale documentazione è conservata come da § 7.
4. Al fine di attestare il momento in cui si è venuti a conoscenza della violazione, RPD segnala la violazione a mezzo email al Titolare del trattamento Formez PA, inviando adeguate informazioni circa la sua natura e gli esiti della valutazione del rischio di cui sopra, nonché anticipando che sta procedendo alla notifica al Garante.

5.4. Notifica della violazione dei dati personali all'autorità di controllo

La normativa prevede che, non appena si viene a conoscenza di una violazione dei dati personali che presenti un rischio di qualsiasi livello superiore al livello “basso” per i diritti e le libertà delle persone coinvolte, è obbligatorio effettuare la notifica all’Autorità.

Per le violazioni così identificate, RPD con il supporti di RAID, redige il documento di notifica della violazione, compilando l’apposito modello presente sul sito dell’Autorità, riprodotto in Allegato 2 “Notifica”, e la invia all’Autorità di controllo tramite posta elettronica certificata (PEC) all’indirizzo PEC della stessa Autorità (dcrt@pec.gpdp.it).

L’invio avviene entro 72 ore dal momento in cui il titolare del trattamento ne è venuto a conoscenza (tale momento si identifica con l'invio della email al Presidente, anche con funzioni di Direttore Generale), a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all’Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il documento di notifica contiene almeno i seguenti elementi:

- la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento

per porre rimedio alla violazione;

- i motivi del ritardo, qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore;
- eventualmente, una dichiarazione sulla mancanza di alcune delle informazioni necessarie e un impegno a fornire, il prima possibile, le informazioni aggiuntive, in una o più fasi successive.

5.5. Comunicazione della violazione dei dati personali a interessato/i

Nel caso di accertamento di una violazione dei dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, come valutato secondo quanto indicato al § 5.2, RPD comunica la violazione all'interessato.

La comunicazione non è richiesta se è soddisfatta una delle seguenti condizioni:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

La comunicazione contiene almeno i seguenti elementi:

- la natura della violazione dei dati personali, descritta con linguaggio semplice e chiaro;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione.

Lo schema di comunicazione è riportato in Allegato 3.

Per la comunicazione, è possibile identificare uno o più canali di comunicazione, a seconda delle circostanze, quali email, SMS, posta, comunicati pubblicitari, banner o notifiche su siti web, scegliendo il canale che massimizza la probabilità che tutti gli interessati siano raggiunti dal messaggio.

5.6. Documentazione della violazione

Per ogni violazione di cui sia accertata l’esistenza, RPD compila il “Registro delle violazioni”, che riporta:

- numerazione progressiva;
- data di rilevazione;
- area/processo interessato dalla violazione;
- descrizione della violazione;
- categorie di interessati in questione;
- numero approssimativo di interessati in questione;
- categorie di registrazioni dei dati personali in questione;
- numero approssimativo di registrazioni dei dati personali in questione;
- cause della violazione;
- conseguenze della violazione;
- misure per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi, con indicazione delle responsabilità e dei tempi per l’attuazione delle misure;
- elementi a supporto della valutazione del rischio: livello di gravità, livello di probabilità, livello di rischio derivante;
- necessità della notifica alla Autorità e data/ora della stessa, ove applicabile;
- necessità della comunicazione all’interessato e data/ora della stessa, ove applicabile;
- verifica dell’attuazione delle misure;
- verifica dell’efficacia delle misure.

Ad integrazione di quanto riportato nel registro, RPD raccoglie e conserva tutti i documenti relativi ad ogni violazione, compresi quelli inerenti le circostanze ad essa relative, le sue

conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è resa disponibile all'Autorità di controllo per le verifiche di competenza.

5.7. Controlli

Qualora siano identificati più titolari del trattamento (caso di responsabili esterni del trattamento o di titolari autonomi), ruoli e responsabilità tra le parti sono stati definiti preliminarmente con la “Nomina di responsabile esterno del trattamento” ovvero con la “clausola privacy” sottoscritte dal soggetto esterno, per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali.

In questi casi, il titolare del trattamento con il supporto di RPD concorda con i responsabili esterni del trattamento o titolari autonomi le modalità per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali, al fine di garantire il rispetto dei termini di notifica e di comunicazione, di cui il titolare del trattamento resta legalmente responsabile.

6. RIFERIMENTI

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- Decreto Legislativo 30 giugno 2003 n. 196, recante il Codice in materia di protezione dei dati personali e provvedimenti adottati dall’Autorità Garante per la protezione dei dati personali;
- Best practices di settore sviluppatesi alla luce del Codice e della giurisprudenza del Garante;
- Linee guida sulla notifica delle violazioni di dati personali ai sensi del Regolamento 679/2016 (WP250), adottate dal Gruppo di lavoro Articolo 29 (“WP29”), in via definitiva, il 6 febbraio 2018;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento “possa presentare un rischio elevato” ai sensi

del Regolamento 2016/679 (WP248), adottate dal WP29, in via definitiva, il 4 ottobre 2017;

- Linee guida sui responsabili della protezione dei dati (WP243), adottate dal WP29, in via definitiva, il 5 aprile 2017;
- Dichiarazione relativa al ruolo di un approccio basato sul rischio nel quadro normativo in materia di protezione dati (WP218), adottata dal WP29 il 30 maggio 2014;
- Raccomandazioni per una metodologia della valutazione della gravità delle violazioni di dati personali, adottate dalla European Union Agency for Network and Information Security (ENISA) il 20 dicembre 2013.

7. ARCHIVIAZIONE

Gli allegati “Notifica” e “Comunicazione” e tutti i documenti relativi alle notifiche ed alle comunicazioni sono archiviati da RPD sul sistema di archiviazione documentale di Formez PA. Il “Registro delle violazioni” e il documento “Scenari di Data Breach” sono archiviati da da RPD sul sistema di archiviazione documentale di Formez PA.

8. ALLEGATI

Allegato 1 - Registro delle violazioni

Allegato 2 – Modello di notifica

Allegato 3 – Comunicazione

Allegato 4 – Scenari di Data breach

Allegato 5 – Modello semplificato